REMARKS

Claims 1-5, 8-14, and 17-23 are pending. By this amendment, claims 21-23 are canceled, claims 1, 8-10, 12, 17-18, and 20 are amended, and new claims 24-25 are added. No new matter is introduced. Support for the amendments and new claims may be found at least at page 5, line 5 to page 6, line 27, page 9, line 1-3, and page 9, lines 14-17 of the specification. Reconsideration and allowance of all pending claims is respectfully requested in view of the preceding amendments and following remarks.

Claim Rejections Under 35 U.S.C. §112

Claims 22-23 are rejected under 35 U.S.C. §112, first paragraph. Claims 22-23 are cancelled, rendering the rejection of claims 22-23 moot.

Claim Rejections Under 35 U.S.C. §102

Claims 1-5, 8-14, and 17-21 are rejected under 35 U.S.C. §102 (e) over U.S. Patent 6,064,813 to Sitbon et al. (hereafter Sitbon). This rejection is respectfully traversed.

Claim 21 has been cancelled, rendering the rejections of claim 21 moot.

Sitbon is directed to an application integration tool for integrating applications into a data processing platform. However, Sitbon does not disclose or suggest "assigning the tools to roles by a trusted user via an authorization model associated with the SCM module; and assigning the roles to a plurality of users via the authorization model, wherein the plurality of users are, depending upon the roles assigned, selectively authorized to execute the tools associated with the roles on nodes in a network; ... determining if a user is authorized to run the tools on each of the nodes in the network," as recited in amended claim 1.

The amendments to claim 1 find support at least at page 5, line 5 to page 6, line 27 of the present application:

> An SCM authorization model supports the notion of assigning to users the ability to run a set of tools on a set of nodes ... Each role may have one or more tools and each tool may belong to one or more roles. When users are given the authority to perform some limited set of functionality on one or more nodes, the authorization is done based upon roles and not on tools ... When a user attempts to run a tool on a node, the user may need to be checked to determine if the user is authorized to fulfill a certain role on the node and if that role contains the tool.

In addition, Figure 2 of the present application further illustrates the relationships between users, roles, nodes, and tools. Sitbon's method does not create a tool definition file by using an authorization model that assigns tools to associated roles and assigns tool enabled roles to different users. Furthermore, Sitbon's method does not check if a user is authorized

to run a tool on each of the nodes requested using the authorization model. Therefore, Sitbon does not disclose or suggest all of the features of amended claim 1, and amended claim 1 is allowable.

Claims 2-5 and 8-11 are allowable at least because they depend from allowable claim 1 and for the additional features they recite.

Regarding claim 12, for at least the same reason as stated above with respect to claim 1, Sitbon does not disclose or suggest "a module for creating a tool definition file ... comprising: roles that are assigned to users and that define which tool the users can run; and an authorization model that assigns the roles to the users and authorizes the users to run tools on nodes based on the roles assigned to the users, wherein the users are, depending upon the roles assigned, selectively authorized to execute the tools associated with the roles on the nodes in a network; ... a module for determining if a user is authorized to run the tools on each of the nodes in the network," as recited in amended claim 12. Since Sitbon does not disclose or suggest all of the elements of amended claim 12, claim 12 is allowable.

Claims 13-14 and 17-19 are allowable at least because they depend from allowable claim 12 and for the additional features they recite.

Regarding claim 20, for at least the same reason as stated above with respect to claim 1, Sitbon does not disclose or suggest "assigning the tools to roles by a trusted user via an authorization model associated with the SCM module; and assigning the roles to a plurality of users via the authorization model, wherein the plurality of users are, depending upon the roles assigned, selectively authorized to execute the tools associated with the roles on nodes in a network; ... determining if a user is authorized to run the tools on each of the nodes in the network," as recited in amended claim 20. Since Sitbon does not disclose or suggest all of the elements of amended claim 20, claim 20 is allowable. Withdrawal of rejections of claims 1-5, 8-14, and 17-20 is respectfully requested.

New claims 24-25 are allowable because they depend from allowable claims 1 and 12, respectively, and for the additional features they recite. For example, Sitbon does not disclose or suggest "automatically assigning newly created tools to a master role via the authorization model associated with the SCM module, wherein a user having the master role on the nodes is capable of running all tools on the nodes in the network," as recited in claim 24.

Similarly, Sitbon does not disclose or suggest "wherein the module for creating the tool definition file further comprises a master role that is automatically provided access to newly created tools, wherein a user having the master role on the nodes is capable of running

all tools on the nodes in the network," as recited in claim 25. Therefore, the new claims are allowable.

In view of the above remarks, prompt examination and allowance are respectfully requested.

Should the Examiner believe that anything further is desired in order to place the application in even better condition for allowance, the Examiner is invited to contact Applicants' undersigned representative at the telephone number listed below.

Respectfully submitted,

Date: **March 24, 2005**

Kelly T. Lee
Registration No. 47,743
Andrews Kurth LLP
1701 Pennsylvania Ave, N.W.
Suite 300
Washington, DC 20006
Tel. (202) 662-2736
Fax (202) 662-2739